MATHEMATICAL AND COMPUTATIONAL SCIENCES DIVISION
AND COMPUTER SECURITY DIVISION
JOINT COLLOQUIUM

A TALK ON QUANTUM CRYPTOGRAPHY
OR
HOW ALICE OUTWITS EVE

Samuel J. Lomonaco, Jr.
Dept. of Computer Science and Electrical Engineering
University of Maryland Baltimore County

Tuesday, September 21, 1999 at 10:30 a.m.
Room 618, NIST North (820)

ABSTRACT

Alice and Bob wish to communicate without the archvillainess Eve eavesdropping on their conversation. Alice, decides to take two college courses, one in cryptography, the other in quantum mechanics. During the courses, she discovers she can use what she has just learned to devise a cryptographic communication system that automatically detects whether or not Eve is up to her villainous eavesdropping. Some of the topics discussed are Heisenberg's Uncertainty Principle, the Vernan cipher, the BB84 and B92 cryptographic protocols. The talk ends with a discussion of some of Eve's possible eavesdropping strategies, opaque eavesdropping, translucent eavesdropping, and translucent eavesdropping with entanglement.

For further information, contact: Bill Mitchell (301) 975-3808.